



QUALYS SECURITY CONFERENCE 2018

# Regaining Our Lost Visibility

**Sumedh Thakar**

Chief Product Officer, Qualys, Inc.



# IT Transformation

## Infrastructure & Application

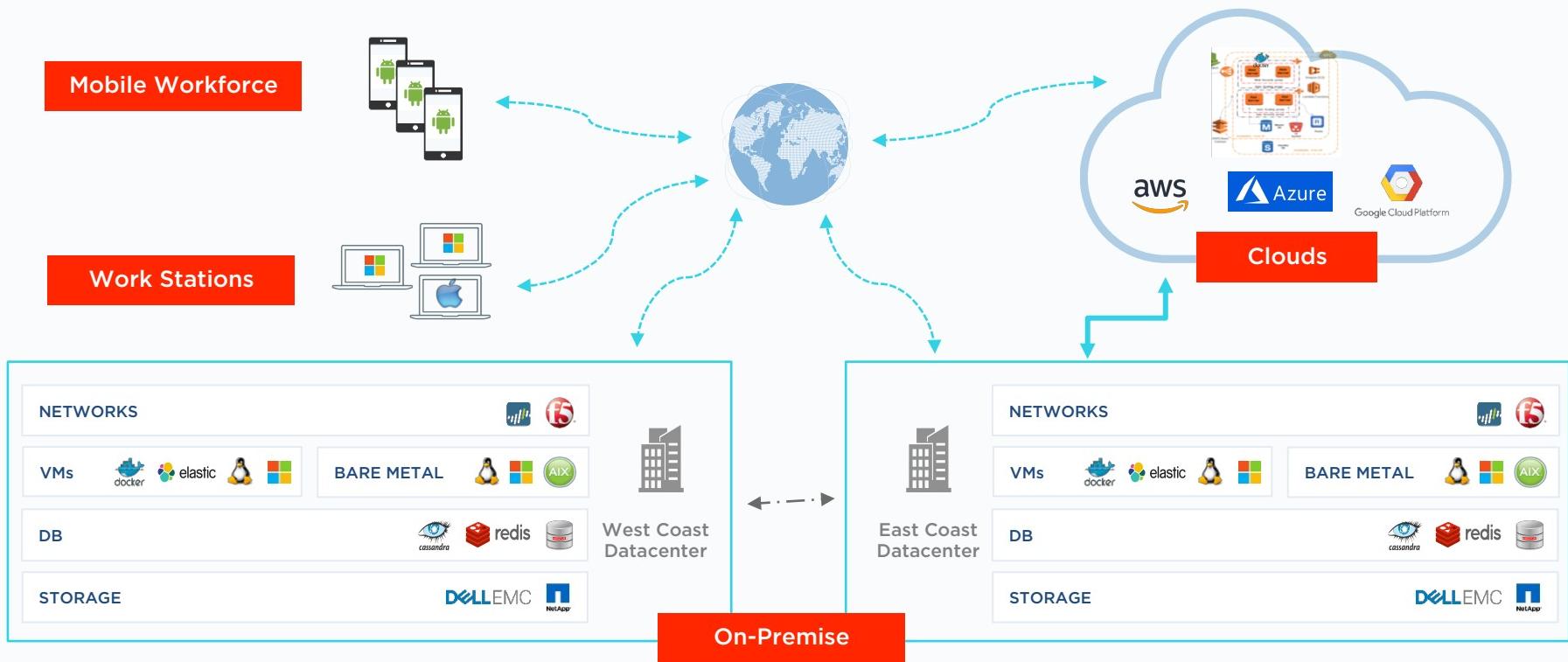
# Digital Transformation

Holistic Transformation of Business to Digital

Cloud, Containers, IaaS, PaaS, OT, IIoT, IoT, Mobility, Web apps, APIs, Mobile Apps



# Hybrid Cloud Overview Architecture



# Containers

Real game changer

Hypervisor disappearing, bare metal is back

Kubernetes Infrastructure-as-code

Container-as-a-Service AWS Fargate

AWS Lambda function-as-a-service, serverless!

Kubefed?

“Priceline” for Containers?

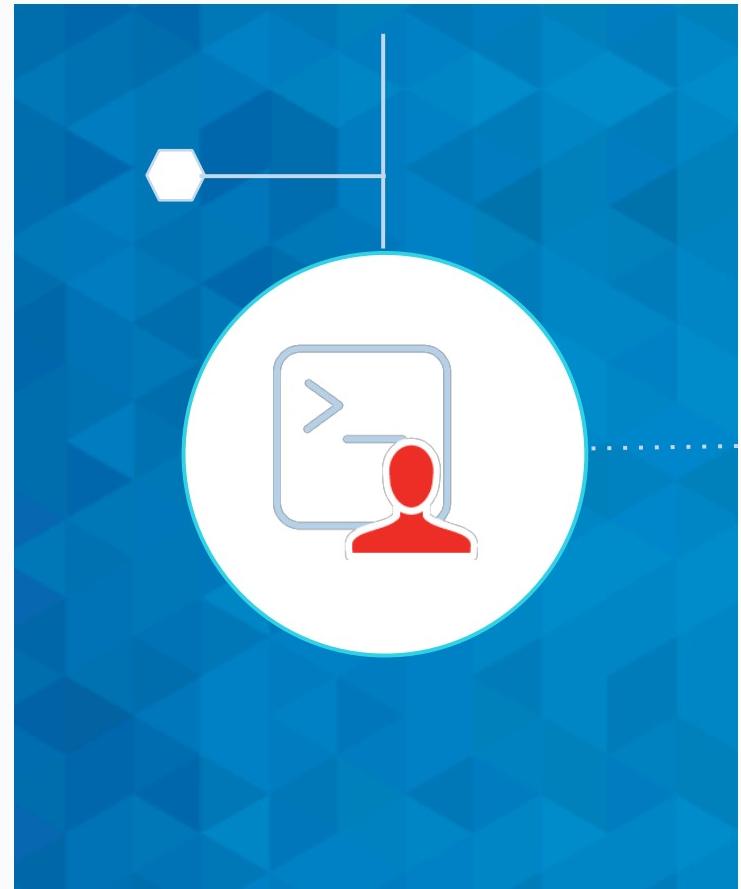


# DevOps

This is real and highly contagious

Developer decides how infrastructure runs in production

Speeds up significantly how fast code goes to production



# On-Prem

Shrinking Datacenter Footprint

Increasing OT & IIoT

Corp IT - more distributed & mobile

More IoT!



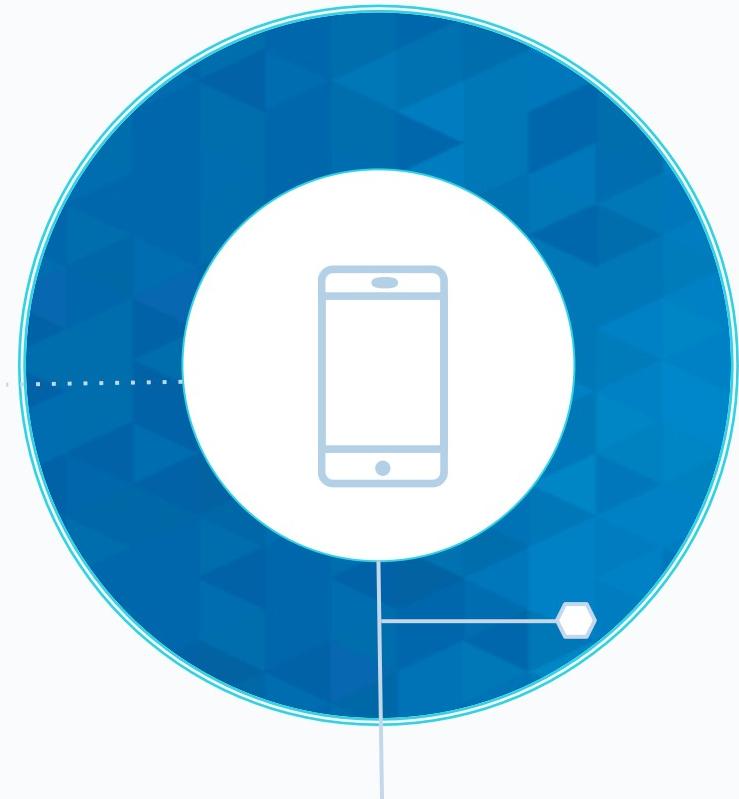
# Enterprise Mobility != BYoD

Enterprise owned handheld devices

Indispensable to modern business

Running apps handling sensitive  
business & consumer data

Mobile!



# Web Apps & APIs

Web Apps for the humans

APIs for the inhumans

Wide window into all your data

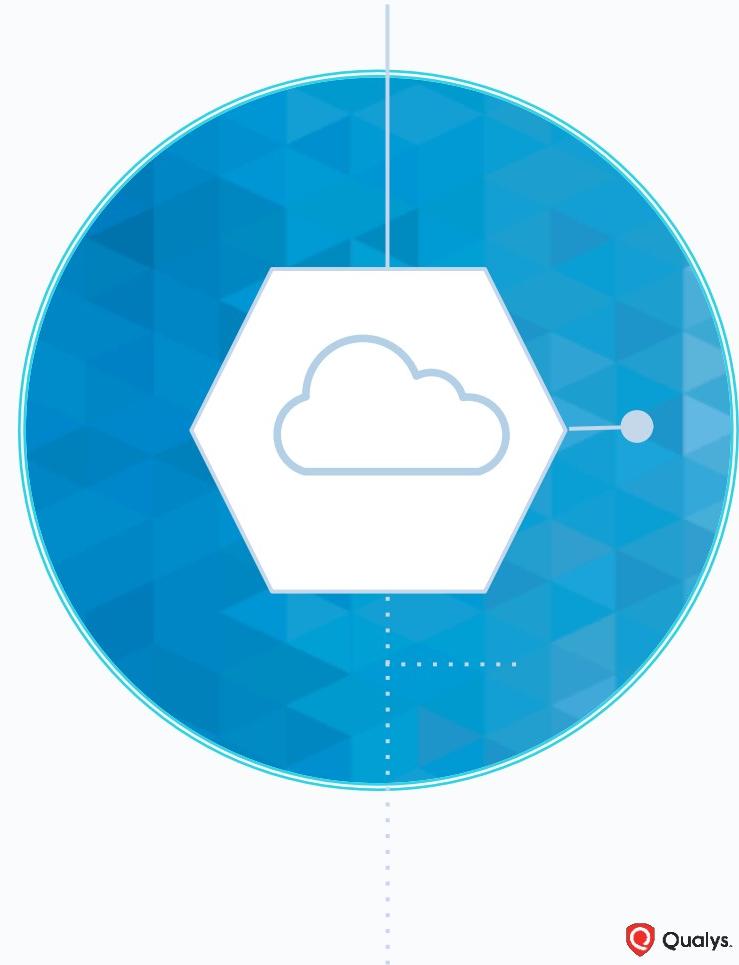


# SaaS

More aaS everywhere

No infrastructure to manage

No Applications to code or manage



# SaaS





# Security



IBM PC AT

# November 13, 1984

PC Magazine about IBM PC AT

“The AT provides the first real system for allowing executives to sleep at night:

A hard-to-duplicate ‘tubular’ key locks all but key holders out of the system”



# 34 years later

No magic key = No sleep at night!

Same challenges x 10

No visibility across global hybrid infrastructure

Still need to do Vulnerability & Configuration management

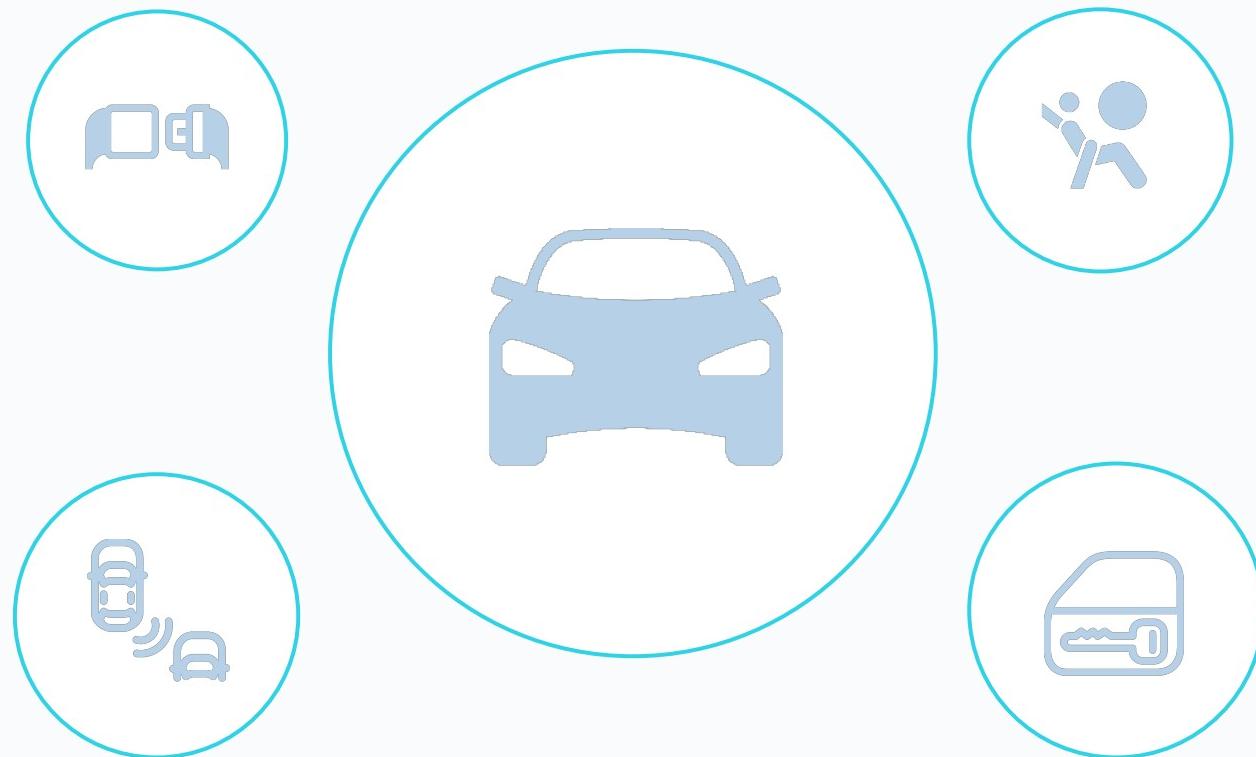
Still need to monitor integrity of systems(?)

More data incoming into “SIEM” deployments

Basically no visibility to respond

Compliance demands on new infrastructure





# Future of Security

Transparent Orchestration

Built-in Automation the only real solution

Starts in DevOps

New generation of Security Analytics platforms





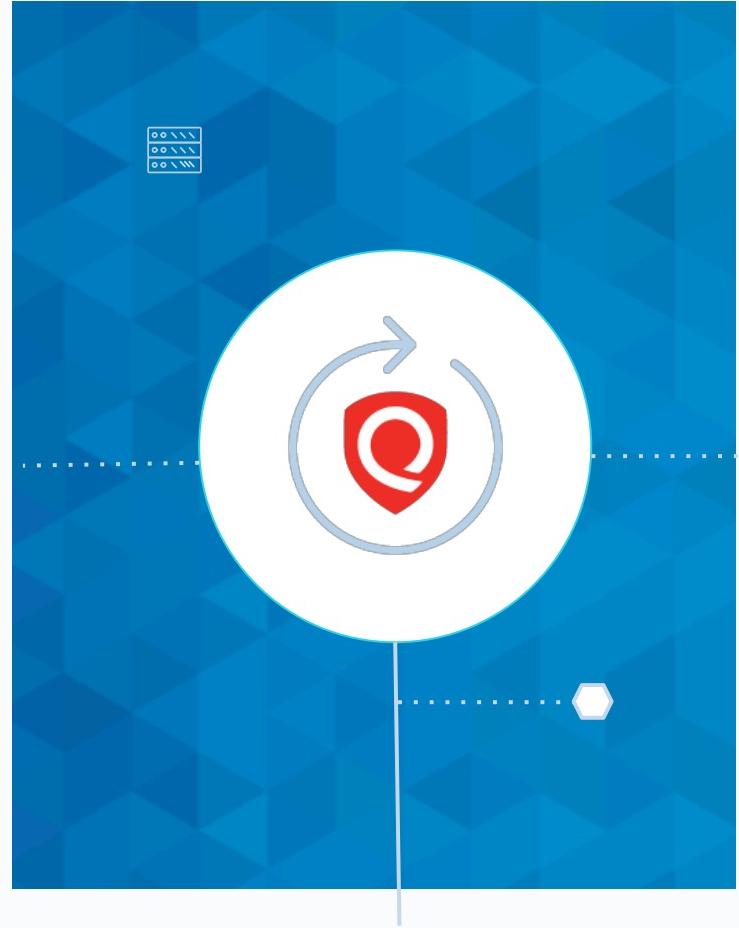
Qualys

# Qualys Platform Approach

Embracing our own Digital Transformation

Massive expansion of backend for visibility – **620 Billion** security datapoints indexed

Comprehensive coverage of sensors – scanners, agents, cloud connectors, container sensors, passive sniffers and mobile agents



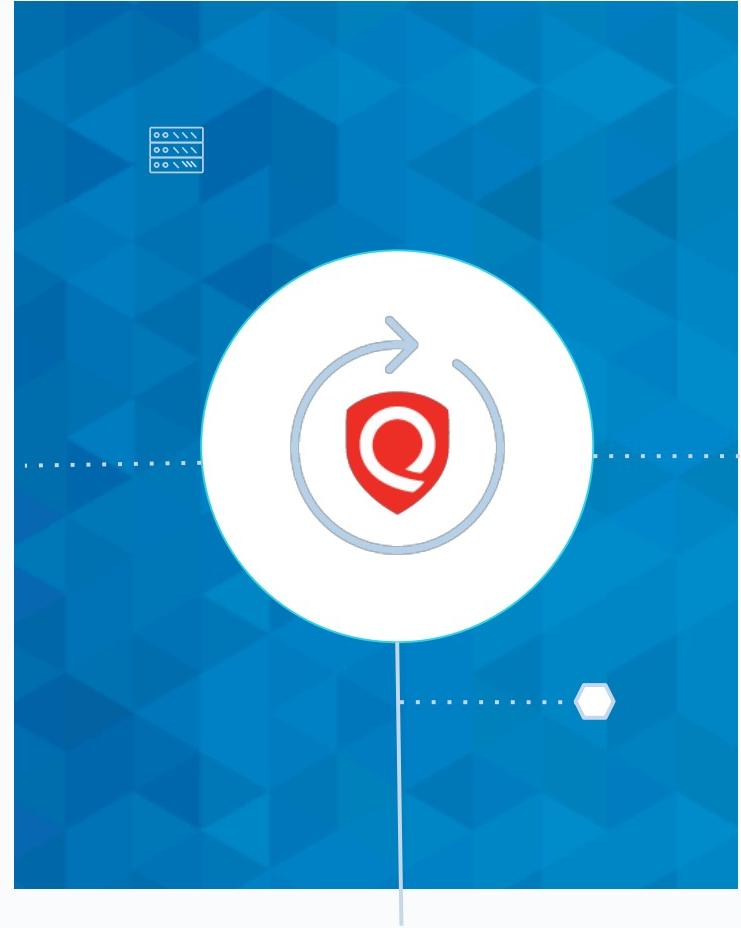
# Qualys Platform Approach

Extending solutions into  
remediation & response

Building dedicated Data science  
team

Rapid expansion of R&D org

Key technology acquisitions &  
Investments



# Acquisitions & Investments

<b>Nevis</b>	Passive Scanning & Secure Access Control
<b>Netwatcher</b>	Event Correlation Platform
<b>1Mobility</b>	Enterprise Mobility
<b>Layered Insight</b>	Built-in Runtime Container Security
<b>42Crunch Investment</b>	API Security
<b>Frog 1</b>	
<b>Frog 2</b>	

# Qualys Cloud Apps

## ASSET MANAGEMENT

### Asset Inventory

Maintain full, instant visibility of all your global IT assets

### CMDB Sync

Synchronize asset information from Qualys into ServiceNow CMDB

### Cloud Inventory

Inventory of all your cloud assets across AWS, Azure, GCP and others

### Certificate Inventory

Inventory of TLS/SSL digital certificates on a global scale

## IT SECURITY

### Vulnerability Management

Continuously detect and protect against attacks, anytime, anywhere

### Threat Protection

Pinpoint your most critical threats and prioritize patching

### Continuous Monitoring

Alerts you in real time about network irregularities

### Indication of Compromise

Continuously monitor endpoints to detect suspicious activity

### Container Security

Discover, track, and continuously protect containers

### Certificate Assessment

Assess all your digital certificates for TLS/SSL vulnerabilities

## COMPLIANCE MONITORING

### Policy Compliance

Assess security configurations of IT systems throughout your network

### PCI Compliance

Automate, simplify and attain PCI compliance quickly

### File Integrity Monitoring

Log and track file changes across global IT systems

### Security Configuration Assessment

Automate configuration assessment of global IT assets

### Cloud Security Assessment

Get full visibility and control across all public cloud instances

### Security Assessment Questionnaire

Minimize the risk of doing business with vendors and other third parties

## WEB APPLICATION SECURITY

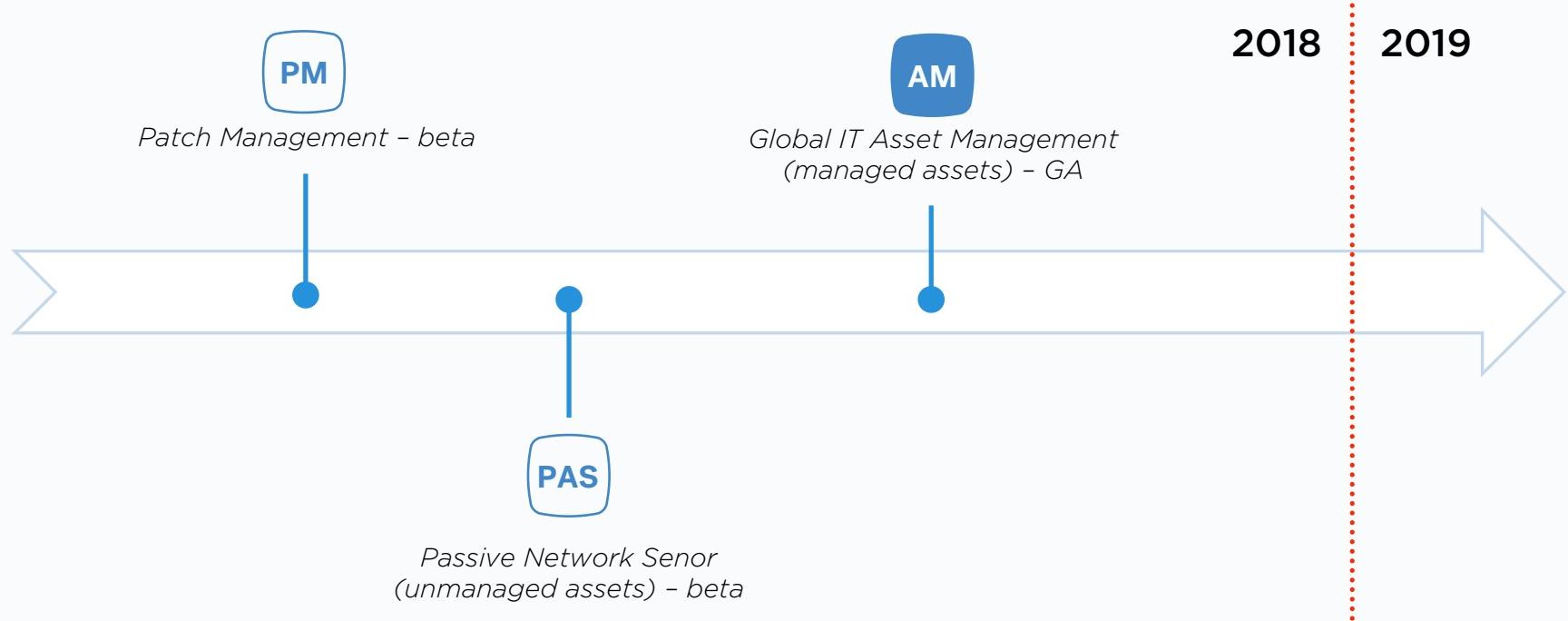
### Web Application Scanning

Secure web applications with end-to-end protection

### Web Application Firewall

Block attacks and virtually patch web application vulnerabilities

# Q4 2018 – more apps to come



# 2019 – even more apps to come!

Secure Enterprise Mobility

Secure Access Control

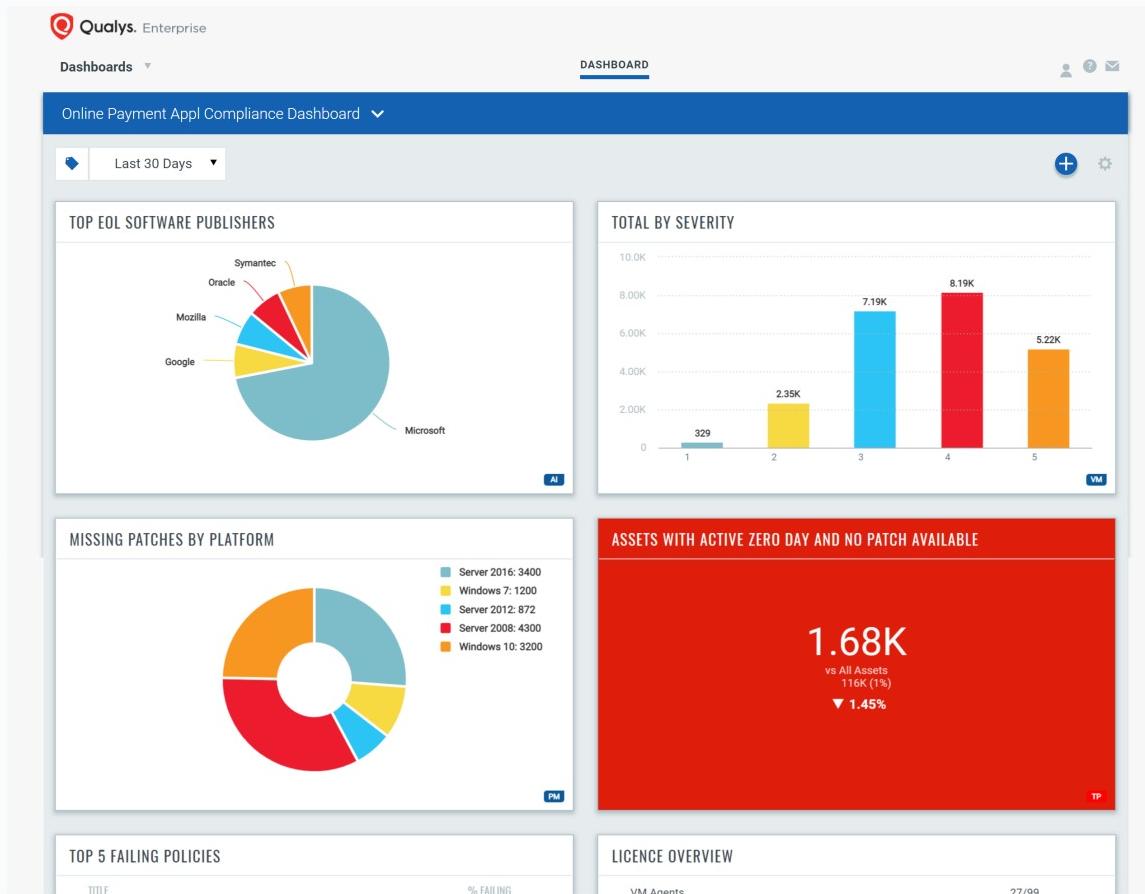
API Security

Software Composition Analysis

Breach and Attack Simulation

Security Data Lake & Correlation Platform

# Unified Dashboards





**DEMO**



**It's the Platform!**  
(a real one)

# Qualys Cloud Platform

Looking Under the Hood: What Makes Our Cloud  
Platform so Scalable and Powerful

# Cloud Platform Environment

## Security at scale on hybrid clouds

**15+ products** providing  
comprehensive suite of security  
solutions

**10,300+ customers**

**7 shared cloud platforms** across  
North America, Europe & Asia

**70+ private clouds platforms**  
deployed globally... on-prem, AWS,  
Azure, GCP

**16+ PB storage** and **16,000 cores**



# Cloud Platform Highlights

**1+ trillion** security events annually

**3+ billion** scans annually

**2.5+ billion** messages daily across Kafka clusters

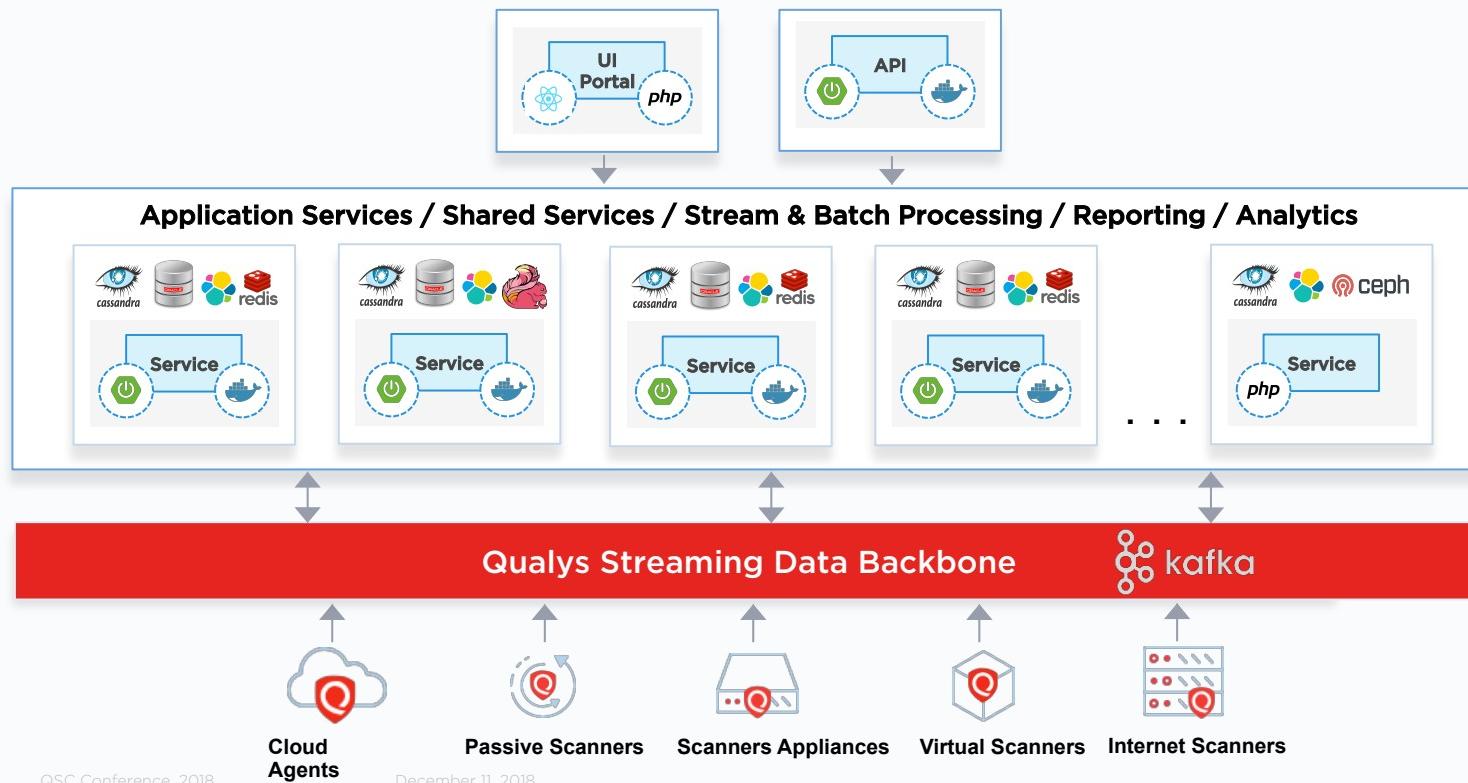
**620+ billion** data points indexed in our Elasticsearch clusters

Unprecedented **2-second** visibility



# Qualys Cloud Platform

## Sensors, Data Platform, Microservices, DevOps



# Qualys Sensor Platform

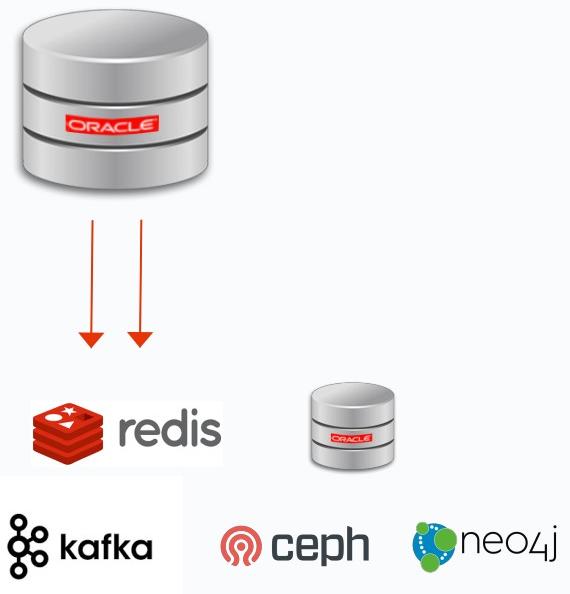
## Scalable, self-updating & centrally managed

Physical	Virtual	Cloud/Container	Cloud Agents	Passive	API
					
Legacy data centers Corporate infrastructure Continuous security and compliance scanning	Private cloud infrastructure Virtualized Infrastructure Continuous security and compliance scanning	Commercial IaaS & PaaS clouds Pre-certified in market place Fully automated with API orchestration Continuous security and compliance scanning	Light weight, multi-platform On premise, elastic cloud & endpoints Real-time data collection Continuous evaluation on platform for security and compliance	Passively sniff on network Real-time device discovery & identification Identification of APT network traffic Extract malware files from network for analysis	Integration with Threat Intel feeds CMDB Integration Log connectors

# Data Platform-as-a-Service

Right database for the right use case

- Highly scalable architecture
- Predictable performance at scale
- Distributed and fault-tolerant
- Multi-datacenter support
- Open-source
- Commodity hardware



# Data Platform-as-a-Service



**Kafka**

Asynchronous,  
event-driven  
architecture

Foundation for  
Qualys Cloud  
Platform

Over 2.5 billion  
messages per day



**Elasticsearch**

Search for anything  
Over 620 billion  
data points indexed

Estimating about 1  
trillion data points  
by year end



**Cassandra**

Low latency  
storage  
Source of truth for  
data across  
multiple products



**Redis**

In-memory cache  
Improved system  
performance for  
frequently  
accessed data



**Ceph**

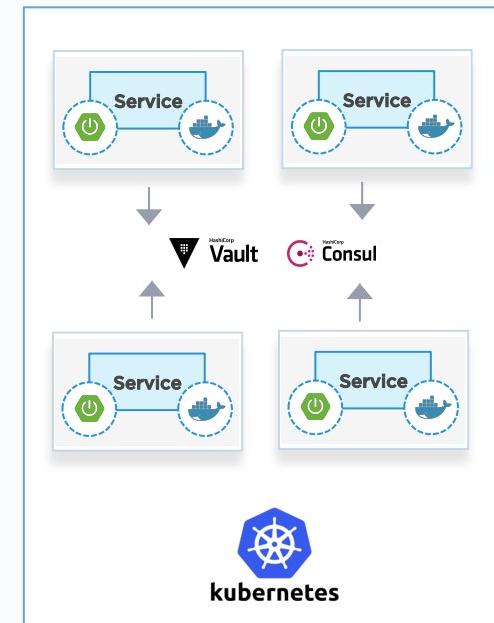
Object storage  
Moving Oracle and  
in-house blob  
storage into Ceph

# Microservices & Cloud Native Architectures

## Reduce risk and ship faster

Change how we design and build applications and services

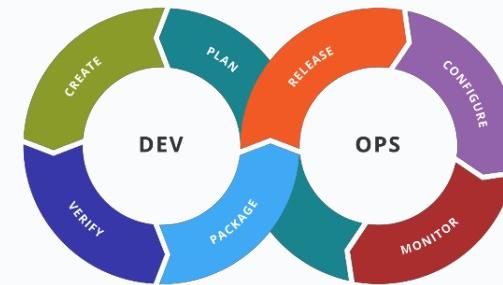
- Monoliths to microservices
- Well defined APIs
- Packaged in containers
- Deployed on elastic infrastructure
- 12-Factor apps
- CI/CD, Service Registry, Config Servers



# DevOps – Increased Efficiency

Goal is to make software delivery vastly more efficient

Supporting about 80 shared and private cloud deployments



# Automation - Infrastructure as Code

Treat systems running your software as if they themselves are software

Automate

- Infra provisioning
- Configuration management
- Deployments...

....all using code



# Monitoring Systems - Observability

Centrally monitor across all platforms using a single-pane view

End-to-end monitoring using

- Time series metrics
- Distributed tracing
- Log aggregation & analytics
- Alerting

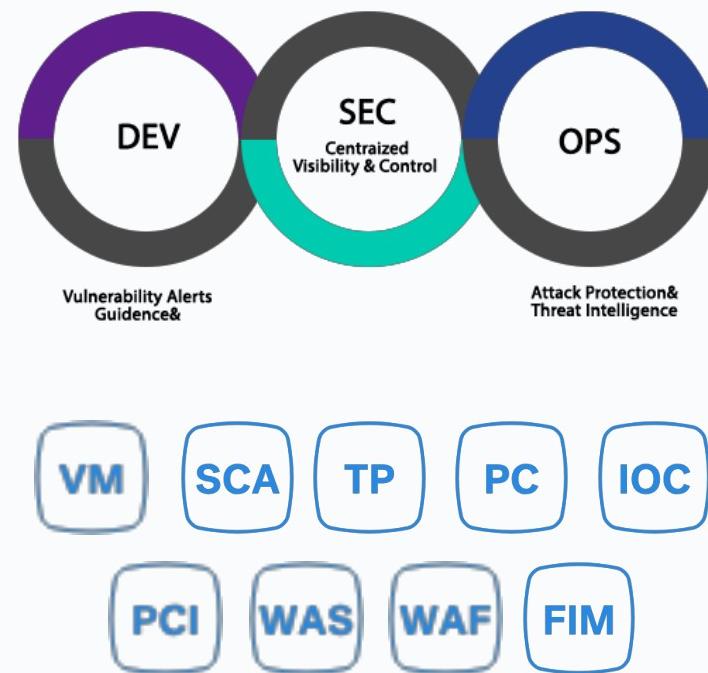


# Integrated Security - DevSecOps

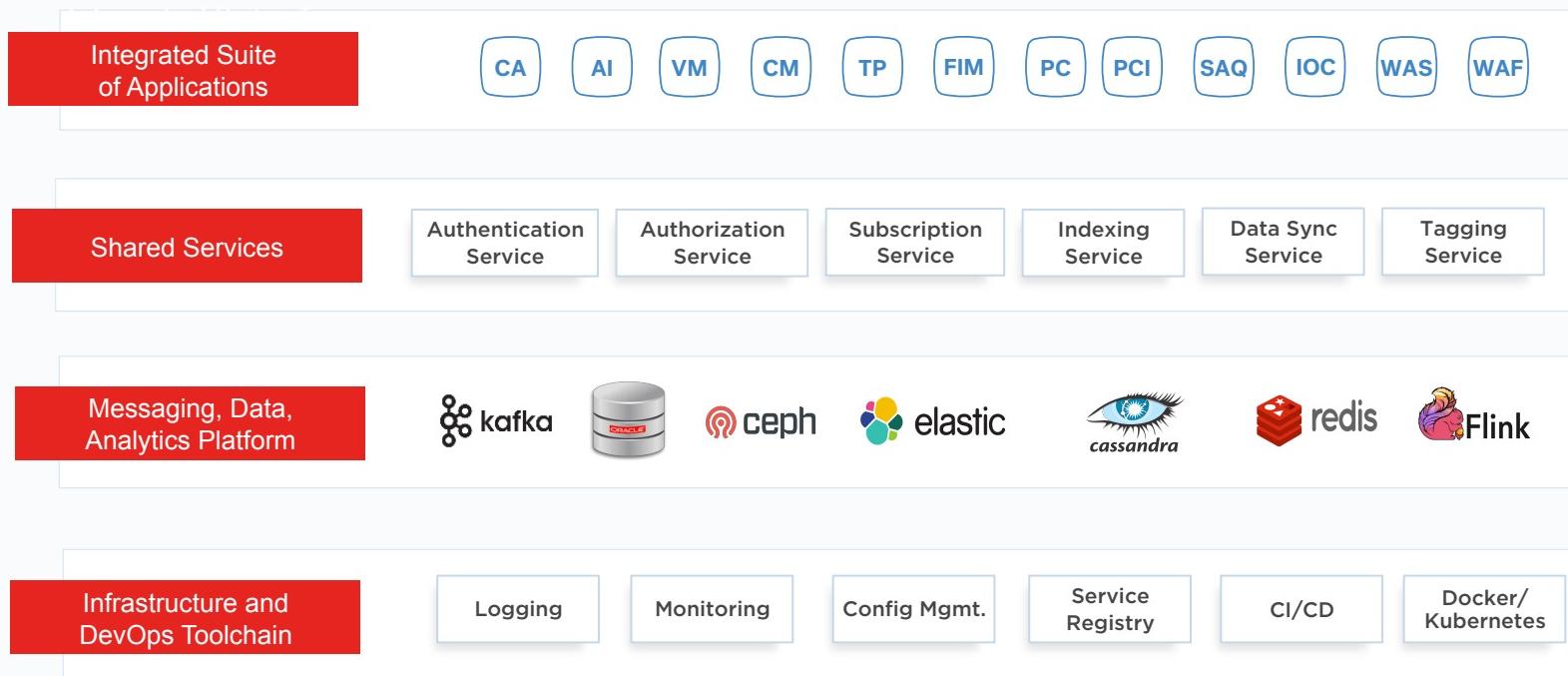
Built-in security practices  
across the DevOps lifecycle

Qualys-on-Qualys

- Manage vulnerabilities
- Comply with policies
- Secure and shield web apps
- Validate file integrity
- Monitor systems



# Qualys Cloud Platform



# Qualys Cloud Applications

## ASSET MANAGEMENT

### Asset Inventory

Maintain full, instant visibility of all your global IT assets

### CMDB Sync

Synchronize asset information from Qualys into ServiceNow CMDB

### Cloud Inventory

Inventory of all your cloud assets across AWS, Azure, GCP and others

### Certificate Inventory

Inventory of TLS/SSL digital certificates on a global scale

## IT SECURITY

### Vulnerability Management

Continuously detect and protect against attacks, anytime, anywhere

### Container Security

Discover, track, and continuously protect containers

### Threat Protection

Pinpoint your most critical threats and prioritize patching

### Certificate Assessment

Assess all your digital certificates for TLS/SSL vulnerabilities

### Continuous Monitoring

Alerts you in real time about network irregularities

### Indication of Compromise

Continuously monitor endpoints to detect suspicious activity

## COMPLIANCE MONITORING

### Policy Compliance

Assess security configurations of IT systems throughout your network

### Cloud Security Assessment

Centralize security and control across all public cloud instances

### PCI Compliance

Automate, simplify and attain PCI compliance quickly

### Security Assessment Questionnaire

Minimize the risk of doing business with vendors and other third parties

### File Integrity Monitoring

Log and track file changes across global IT systems

### Security Configuration Assessment

Automated configuration assessment of global IT assets

## WEB APPLICATION SECURITY

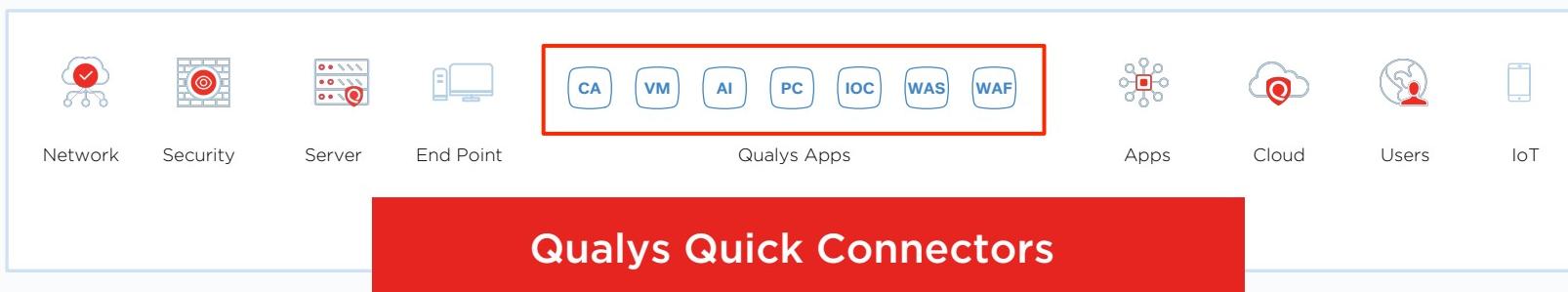
### Web Application Scanning

Applications with end-to-end protection

### Web Application Firewall

Block attacks and virtually patch web application vulnerabilities

# Advanced Correlation & Analytics





QUALYS SECURITY CONFERENCE 2018

# Thank You

**Sumedh Thakar**

[sthakar@qualys.com](mailto:sthakar@qualys.com)